#### card of course

|  |  |
| --- | --- |
| Subject name | * + - 1. **IT security audit**
 |

**1. The placement of the subject in the study system**

|  |  |
| --- | --- |
| 1.1. Field of study | **Computer science** |
| 1.2. Form and path of study | **Full-time/Part-time** |
| 1.3. Level of education | **First-cycle studies** |
| 1.4. Study profile | **Practical** |

|  |  |
| --- | --- |
| 1.5. Specialty | **Cybersecurity and computer forensics** |
| 1.6. Subject Coordinator | **Dr inż. Mateusz Górka; mgr inż. Mateusz Musiałek** |

**2. General characteristics of the subject**

|  |  |
| --- | --- |
| 2.1. Belonging to a subject group | **Optional/practical** |
| 2.2. Number of ECTS | **4** |
| 2.3. Language of lectures | **English** |
| 2.4. Semesters in which the subject is taught | **V** |
| 2.5.Criteria for selecting course participants | **For specializations: Cybersecurity and computer forensics** |

1. **learning outcomes and course delivery**
	1. **Subject Objectives**

|  |  |
| --- | --- |
| **No.** | **Subject Objectives** |
|
| C1 | Familiarization with the issue of computer system security, the applicable regulations and ISO standards in this area, and the issues of creating computer system security policies, principles and procedures. |
| C2 | Familiarization with the most common threats, errors leading to gaps in system security, and techniques for avoiding them. |
| C3 | Acquiring skills in using security analysis tools, monitoring tools, attack detection systems and methods of protection against attacks - supplemented by a discussion of computer forensics issues. |
| C4 | Familiarization with security models and security classes of systems. Obtaining knowledge about authentication models, access control strategies, including in the context of security of communication protocols and application services. |
| C5 | Case study - learning practical methods for selecting and applying appropriate security measures based on a real event - students will learn about the causes of incidents, methods of detecting them and analyzing them. |

* 1. **Subject-specific learning outcomes, divided into knowledge , skills and competences , with reference to the directional learning outcomes**

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Description of subject learning outcomes** | **Reference to directional effects****learning (symbols)** | **Method of implementation (mark "X")** |
| **ST** | **NST** |
| **Classes at the University** | **Activities on the platform** | **Classes at the University** | **Activities on the platform** |
| After passing the course, the student knows and understands **the knowledge** |
| W1 | Methods of solving security problems used in computer systems and knows how to apply them. | INF\_W05INF\_W15 |  | X |  | X |
| W2 | principles in the use and design of information systems. |  | X |  | X |
| W3 | Principles of ensuring compliance of the security level of computer systems with legal requirements. |  | X |  | X |
| W4 | Has knowledge of tools used to analyze computer system security. |  | X |  | X |
| W5 | The role of data security and information systems for the functioning of modern society. |  | X |  | X |
| After passing the course, the student is **able** to: |
| U1 | Identify threats to the security of computer systems. | INF\_U13INF\_U25 | X |  | X |  |
| U2 | Select methods and tools for protecting computer systems. | X |  | X |  |
| U3 | Identify security level compliance computer system with legal requirements. | X |  | X |  |
| U4 | Implement a data security system and IT systems. | X |  | X |  |
| After completing the course, the student is ready to take part in **social competences.** |
| K1 | Professional activities in the field of IT security requiring continuous development of knowledge and skills. | INF\_K02INF\_K05 | X |  | X |  |
| K2 | Understanding the consequences and effects of omissions and actions taken in the field of security. | X |  | X |  |
| K3 | Concerned about privacy and data protection. Has ethical awareness. | X |  | X |  |

**3.3. Forms of teaching and their number of hours - Full-time studies (ST), Part-time studies (NST)**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Path** | **Lecture** | **Exercises** | **Design** | **Workshop** | **Laboratory** | **Seminar** | **Lecturer** | **Classes conducted using distance learning methods and techniques in the form of a lecture** | **Other** | **ECTS points** |
| **ST** |  |  |  |  | 30 |  |  | 20 |  | 4 |
| **NST** |  |  |  |  | 15 |  |  | 10 |  | 4 |

**3.4. Content of education** (separately for each form of classes: (W, ĆW, PROJ, WAR, LAB, LEK, OTHER). It should be marked (X) how the given content will be implemented (classes at the university or classes on the e-learning platform conducted using distance learning methods and techniques)

**TYPE OF CLASS: LECTURE**

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Content of the course** | **Reference to subject-specific learning outcomes** | **Method of implementation (mark "X")** |
| **ST** | **NST** |
| **Classes at the University** | **Activities on the platform** | **Classes at the University** | **Activities on the platform** |
| **1.** | Basic issues and definitions in the field of computer system security. The importance of computer system security. | **W1** |  | **X** |  | **X** |
| **2.** | Security Policy. Preparation for the development of a system security policy. Risk analysis, i.e. analysis of resources, threats and vulnerabilities of resources. | **W2, W4** |  | **X** |  | **X** |
| **3.** | Formulation of the policy and development of the document "System Security Policy" on this basis. Basic principles of the security policy. General principles of the policysafety | **W3** |  | **X** |  | **X** |
| **4.** | System security audits.  | **W5** |  | **X** |  | **X** |
| **5.** | Human Factor Safety Audit. Factors increasing risk. | **W5** |  | **X** |  | **X** |
| **6.** | Summary of classes and discussion of grades. |  |  | **X** |  | **X** |

**TYPE OF CLASS: LABORATORY**

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Content of the course** | **Reference to subject-specific learning outcomes** | **Method of implementation (mark "X")** |
| **ST** | **NST** |
| **Classes at the University** | **Activities on the platform** | **Classes at the University** | **Activities on the platform** |
| **1.** | Security of computer systems from the point of view of configuration methods. The importance of computer system security. | **U1, K1** | **X** |  | **X** |  |
| **2.** | Security Policy. Preparation for the development of a system security policy - examples. Risk analysis, i.e. analysis of resources, threats and vulnerabilities of resources. Methods of counteracting threats. | **U2, K1** | **X** |  | **X** |  |
| **3.** | Formulation of the policy and development of the document "System Security Policy" on this basis. Basic principles of the security policy. General principles of the policysecurity – practical examples and methods. | **U3** | **X** |  | **X** |  |
| **4.** | System security audits - preparation and procedures for conducting an IT security audit.  | **U4, K1** | **X** |  | **X** |  |
| **5.** | Human Factors Security Audit. Risk Increasing Factors. Error Vulnerabilities. | **U4, K2, K3** | **X** |  | **X** |  |
| **6.** | Summary of classes and discussion of grades. |  | **X** |  | **X** |  |

**3.5. Methods of verifying learning outcomes** (indication and description of methods of conducting classes and verification of achievement of learning outcomes and method of documentation)

|  |  |  |  |
| --- | --- | --- | --- |
| **Subject Effects** | **Teaching methods** | **Methods of verifying learning outcomes** | **Documentation methods** |
| **KNOWLEDGE** |
| **W1-W5** | informative, conversational lecture with the use of multimedia | Test – passing the lecture | Test sheet |
| **SKILLS** |
| **U1-U4** | Case study, discussions, task completion | Laboratory assessment - students perform professional SWOT analyses of individual parts of the audit, i.e. software legality audit, hardware audit and its records, security audit of the security technologies used. | Assessed work |
| **SOCIAL COMPETENCES** |
| **K1-K3** | Case study, discussions, task completion | Laboratory assessment - students perform professional SWOT analyses of individual parts of the audit, i.e. software legality audit, hardware audit and its records, security audit of the security technologies used. | Assessed work |

**3.6. Assessment criteria for the achieved learning outcomes**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Learning effect** | **For a grade of 3 or " zal ."****the student knows and understands/is able to/is ready to** | **For a grade of 3.5, the student knows and understands/is able to/is ready to** | **For a grade of 4, the student knows and understands/is able to/is ready to** | **For a grade of 4.5, the student knows and understands/is able to/is ready to** | **For a grade of 5, the student knows and understands/is able to/is ready to** |
| W | 51-60% of knowledge indicated in learning outcomes | 61-70% of knowledge indicated in learning outcomes | 71-80% of knowledge indicated in learning outcomes | 81-90% of knowledge indicated in learning outcomes | 91-100% of knowledge indicated in learning outcomes |
| U | 51-60% of skills indicated in learning outcomes | 61-70% of skills indicated in learning outcomes | 71-80% of skills indicated in learning outcomes | 81-90% of skills indicated in learning outcomes | 91-100% of skills indicated in learning outcomes |
| K | 51-60% of skills indicated in learning outcomes | 61-70% of skills indicated in learning outcomes | 71-80% of skills indicated in learning outcomes | 81-90% of skills indicated in learning outcomes | 91-100% of skills indicated in learning outcomes |

**3.7. Literature**

**Basic**

1. IT Auditing Using Controls to Protect Information Assets – Chris Davis, Mike Schiller, Kevin Wheeler
2. Stallings William, Brown Lawrie, Bezpieczeństwo systemów informatycznych : zasady i praktyka. T. 1, Helion, Gliwice, 2023
3. Stallings William, Brown Lawrie, Bezpieczeństwo systemów informatycznych : zasady i praktyka. T. 2, Helion, Gliwice,
4. Diogenes Yuri, Ozkaya Erdal, Cyberbezpieczeństwo : strategie ataku i obrony: jak osiągnąć najwyższy możliwy stan zabezpieczeń systemu informatycznego, Helion, Gliwice, 2023

**Supplementary**

1. National Institute of Standards and Technology; An Introduction to Information Security” (NIST SP 800-12) - National Institute of Standards and Technology (NIST); CreateSpace; Scotts Valley 2017
2. Liderman Krzysztof, Bezpieczeństwo informacyjne : nowe wyzwania, PWN, Warszawa, 2017
3. Liderman Krzysztof, Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN, Warszawa, 2009
4. Tarapata Jolanta (red.), Odporność organizacji : cyfryzacja, bezpieczeństwo, innowacje, Difin, Warszawa, 2022

**4. Student workload - ECTS points balance**

|  |  |
| --- | --- |
| **Types of student activity** | **Student Load** |
| **ST** | **NST** |
| **Classes requiring direct contact between the student and the academic teacher at the university premises** | **50** | **25** |
| Classes included in the study plan | 50 | 25 |
| **Student's own work** | **50** | **75** |
| Ongoing preparation for classes, preparation of project work/presentations/etc. | 25 | 35 |
| Preparation for passing classes | 25 | 40 |
| **TOTAL STUDENT HOURLY LOAD** | **100** | **100** |
| **Number of ECTS points** | **4** | **4** |

|  |  |
| --- | --- |
| Last change date | 30/09/2024 |
| The changes were introduced | INF Education Quality Team |
| The changes were approved | Arkadiusz Gwarda, M.A. |